

REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

By this Amendment, Claims 1, 12 and 14 have been amended to include the features of Claim 2. Claims 3, 4, 5, 9 and 11 have also been amended to place them in better U.S. form. The Abstract has also been amended in accordance with the Examiner's recommendation.

The Office Action rejects claims 1-4, 9-10 and 12-15 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 4,786,790 to Kruse et al (hereinafter "Kruse"); Claims 5, 8 and 11 under 35 U.S.C. § 103(a) as unpatentable over Kruse in view of U.S. Patent No. 4,656,463 to Anders et al. (hereinafter "Anders"); Claim 6 under 35 U.S.C. § 103(a) as unpatentable over Kruse and further in view of U.S. Patent No. 6,167,516 to Camion et al. (hereinafter "Camion"); Claim 7 under 35 U.S.C. § 103(a) as unpatentable over Kruse and further in view of U.S. Patent No. 4,896,261 to Nolan (hereinafter "Nolan"). As will become apparent from the following discussion, the references fail to anticipate or render obvious the claims.

Claim 1 recites, *inter alia*, a method for authenticating a portable object including information processing means and information storage means. The information storage means contains at least one code defining operation steps capable of being executed by the portable object as well as a one-way function. An order is sent to the portable object for executing a calculation of a result by applying to the one-way function at least part of the code and the results input into the implementation of a given operation, the operation being performed successfully only when the portable object is authentic. Comparable amendments have been made to claims 12 and 14 to generally recite that the result is input into the

implementation of a given operation. Claim 9 also generally recites that the result is input into the implementation of the sensitive operation.

As discussed in the specification, an authentication process is generally based on checks made on secret keys stored in portable objects. However, it is possible for hackers to discover these keys. When a secret key is discovered, it is possible to create cloned portable objects that offer the same services as the authentic portable object. However, the cloned portable objects are most often substantially different from the authentic portable objects in terms of their hardware and/or software configuration and in particular, the processing means are different. For example, the programs can be written in different languages, some programs are not the same, and the like. In accordance with Claim 1, at least part of the code that defines operation steps and a result are applied to the one-way function, where the operation is performed successfully only when the portable object is authentic.

Therefore, in the case where the portable object is not authentic, there is a high likelihood that the program code used in the authentication calculation will not be identical to that of an authentic portable object and will result in a bad calculation result, and as a consequence, an incorrect execution of a program operation.

Kruse relates to a data exchange method and system with authentication code comparison. The object of Kruse is to provide a data system such that an unmanipulatable data flow control is guaranteed within the user terminal. The authentication system and method is based on an authentication code, calculated from a secret cipher and a random number. In Kruse, the terminal (KT) and the portable object (KK) both have a memory stored program (P) for controlling data flow. The portable object contains a random number generator and means for selecting parts of the program for controlling data flow based on the output of the random number generator. These parts are selected from the data memory and

the portable object (KK) and in the terminal (KT). Then, both the terminal (KT) and the portable object (KK) calculate an authentication code from the program parts with the assistance of the authentication algorithm and the secret key. A comparison is made between both calculated authentication codes to determine whether both results agree.

As stated on column 2, lines 24-25 of Kruse, the program (P) for data flow control is situated in the customer terminal (KT). It can be checked either by use of a customer card (KK) before inputting the personal identification PIN, or by use of a test chip card. As further discussed on column 2, lines 60-66 of Kruse, the program authentication codes PACv determine whether the results calculated by the customer card (KK) and by the customer terminal (KT) agree.

Kruse fails to teach or suggest the use of parts of any program codes stored on the portable object for use in the calculation of a result used in the authentication process as claimed.

Based at least on this distinction, it is apparent that Independent Claims 1, 9, 12 and 14 are not anticipated nor rendered obvious by Kruse. Furthermore, the claims that depend therefrom are allowable for at least these reasons and the additional feature(s) recited therein. The remaining references, taken either alone or in combination fail to overcome the deficiencies as noted above. An early and favorable Notice of Allowance is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is encouraged to contact Applicants' undersigned representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to deposit account number 50-1165 (Docket No. T2146-907683) and fees not included herein, under 37 CFR §§ 1.16 and 1.17, that may be required by this paper and to credit any overpayment to that Account. A duplicate copy of this page is included for such purpose. If any additional extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.



Date: April 23, 2004

By: Edward J. Kondracki
Registration No. 20,604

Miles & Stockbridge P.C.
1751 Pinnacle Dr., Suite 500
McLean, VA 22102
Phone 703-610-8627
Fax 703-610-8686